Analysing Trust Issues in Cloud Identity Environments

Brian Cusack
Digital Forensic Research Laboratories
AUT University
Auckland, New Zealand
Email: brian.cusack@aut.ac.nz

Eghbal Ghazizadeh
Digital Forensic Research Laboratories
AUT University
Auckland, New Zealand
Email: eghbal.ghazi@aut.ac.nz

Abstract

Trust acts as a facilitator for decision making in environments, where decisions are subject to risk and uncertainty. Security is one of the factors contributing to the trust model that is a requirement for service users. In this paper we ask, What can be done to improve end user trust in choosing a cloud identity provider? Security and privacy are central issues in a cloud identity environment and it is the end user who determines the amount of trust they have in any identity system. This paper is an in-depth literature survey that evaluates identity service delivery in a cloud environment from the perspective of the service user. A trust framework is sought that will provide the end user the capability of evaluating the trust they may have in any service. The analysis resolves the possibility of a single trust value that gives an overall security strength of the cloud identity service. Such a metric can provide informed end user choice. Consideration is also given to the decay or enhancement of the trust value based on user experience and transactions over a period of time.

Keywords Trust, Identity, End user, Frameworks, Metrics

1 Introduction

A trust management framework for assessing the trustworthiness of a cloud identity provider can be developed that aggregates and manages trust-related information from different sources within and without the cloud environment. The proposal is based on the analysis and improvement of existing work, and has a systematic design that helps the cloud end users to find the particular provider that fulfils their requirements. This work differentiates from previous trust management publications, for example Noor et al. (2013), and Roy et al. (2015), by assessing trust for cloud identity management from the perspective of the end-user. Noor et al., (2016) argue that trust and reputation are indispensable conditions for the social conviviality in human societies. Cloud federation environments has similar conditions for interaction where cloud users can join and leave an identity provider frequently. , However, traditional trust solutions have structural difficulties when applied to a cloud environment (Habib, Hauke, Ries, & Mühlhäuser, 2012). Due to the subjective and context-sensitive nature of trust the selection of a cloud provider with fully trusted and appropriate services is one of the most challenging issues in the multi-tenant cloud environment (Ray, Ray, & Chakraborty, 2009). Often Cloud providers have many services that are hosted and tiered for multiple users. As a consequence there can be a variation of services by the one provider. All of these matters impact upon an end user trust level and the decision for use.

Further complications arise as the end user looks for evidence on which to make a decision. Trust relationships between entities in cloud computing are dynamic, uncertain and hard to quantify (Pearson, 2013). The decision maker has to take ownership of the risk and to draw a judgement based on wide variation. The Trust models for cloud identity providers often do not allow for such uncertainty and require improvement by increasing the number of specific attributes taken into account that are relevant when selecting cloud identity providers (Shaikh & Sasikumar, 2015). Common decisions tend to choose the most credible node under one single factor, but ignore the other factors that provide evidence of actual transactions. Such decision-making often lacks a mechanism to evaluate different cloud entities' different quality of service (QoS) requirements (Zheng, Wu, Zhang, Lyu, & Wang, 2013). Furthermore, cloud has many unique features compared to traditional environments that require tools for evaluation before trustworthy evidence can be accumulated, evaluated, and decisions made. In this sense there is a gap to be filled with regard to evidence available to end users for decision-making in cloud environments.

Central to the concern is how to compare each Cloud service based on an agreed set of attributes, and then how to quantify and aggregate them with a meaningful metric (Oliveira et al., 2014). The combination of information from different sources demands multiple criteria decision making (MCDM) (Ramesh & Zionts, 2013). This often requires decision-makers to choose or rank alternatives on the basis of an evaluation of several criteria. Hence, decision making involves managing trade-offs or compromises among a number of criteria that are in conflict with each other (Garg, Versteeg, & Buyya, 2013). The method is related to how much customization should be supported and where the trust values should be aggregated. In the case of QoS, several challenges are found in constructing the model for evaluation and ranking of Cloud identity providers. To establish and measure a Cloud Identity Measurement Index (CIMI) a set of attributes requires continuous updating and adjustment for variation over time. However, without having precise measurement models for each attribute, it is not possible to compare different CSMI. The second challenge is how to rank the Cloud identity based on CIMI attributes. There are two types of QoS requirements which a user can have: functional and non-functional. Some of them cannot be measured easily given the nature of the Cloud environments. Attributes like security and user experience are difficult to quantify. Moreover, to decide which service matches with all the functional and non-functional requirements is a decision problem. It is necessary to think critically before selection, apply the multiple criteria and preserve the independence of relationships. Subsequently, the assigning of weights to trust attributes is necessary in the building of a trust model (Benlian & Hess, 2011).

This introduction section has scoped the problem context and the remainder of the paper is structured to define cloud computing and its related Security, trust and privacy issues. Cloud identity management is then review so that trust models and their mechanisms may be evaluated. To conclude, sixteen currently available trust frameworks are analysed to deliver potential solutions for a singular metric and an end user system architecture for decision-making.

2 Cloud Computing

Cloud computing integrates various computing technologies to provide services to the end users (Wei et al., 2014). Efficient use of businesses resources is one of the main advantages of cloud computing. The charging of the "pay as you use" model is an attractive option for businesses who wish to reduce the cost

of assets and related personnel costs (Aleem & Ryan Sprott, 2012). Cloud computing permits services to be marketed independent of technologies and vendor's so that an end user may efficiently and economically choose, which and what service best suits them (Ali, Khan, & Vasilakos, 2015). The price driver of cloud computing has impacted on even the more recent business models and has initiated fresh rounds of restructuring. The global reach of such opportunities has brought with it concerns regarding security, privacy, monitoring, and trust. These challenges are being taken up by the research community, and solutions are being made available for industry and end users that have negotiated an optimal payback from the resources being invested. A full review of these issues and analysis may be found in Ardqggna & Etisalat (2015).

The NIST definition (NIST, 2013) of cloud computing is widely used to define the concept. In figure 1 the cloud computing scope has four separate descriptions of service provisioning which are common characteristics, essential characteristics, service models, and deployment models.

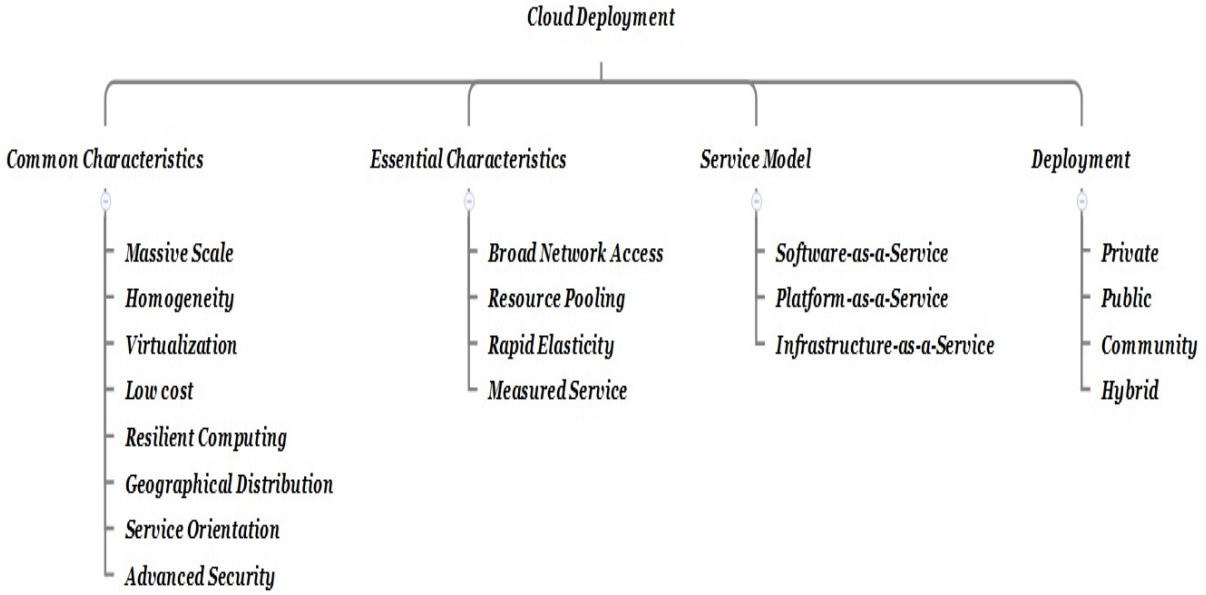

Figure1: Deployment descriptions for cloud (NIST, 2013)

The five essential features of cloud computing differentiate the concept from traditional grid computing by including the scope of Broad network access. This essential characteristic opens the computing grid to a World Wide Web of services. The concept makes available resource pooling, and on-demand self-service, within an economic model that is termed Measured Service. The NIST definition provides a scope of what to expect in cloud computing. However the way the definition is interpreted and implemented is entirely up to a service provider. This is where the key issues and challenges arise. To the end user each of these essential characteristics are desirable and useful for economic advantage. However the service provider has to also act in their own interest to maintain their business in the face of competition and technical challenges. The result can be that the end user may not experience the service they expect. In addition to the NIST description scope, others have developed deployment models that best suit their conception of a commercial opportunity. For example, Alhamazani et al. (2015) described one particular approach named Anything-as-a-Service (XaaS) , which refers to the fact that cloud systems are able to support and offer anything, or everything, in the form of services, ranging from large resources to personal, specific, and granular requirements. Examples include Trust-as-a-Service (TaaS), Identity-as-a-Service (IDaaS), Data-as-a-Service (DaaS), Routing-as-a-Service (RaaS), and Security-as-a-Service (SecaaS). The implication of these developments is for a growing scope of what may be described as cloud computing. The NIST (2013) definition provides adequate scope to be robust in the face of an unfolding concept.

2.1 Cloud Security Issues

Cloud security increases the complexity of traditional computing systems protection by adding multiple layers of design and potential opportunity for vulnerability (Goode et al., 2015). The standard CIA criteria are still required. This implies that a combination of confidentiality, in the prevention of the unauthorized disclosure of information, is required. Integrity, and the prevention of the unauthorized amendment or deletion of information, is required. Similarly the Availability of services and the prevention of the unauthorized withholding of information, is also required (Cabarcos et al., 2012).

Bezzi, Kalavan & Sabetta (2011) resolved security issues in cloud computing environments into six sub-categories, which include:

- How to provide safety mechanisms to monitor or trace the cloud server.
- How to keep data confidentiality for individuals and sensitivity.
- How to avoid a malicious insider's illegal operations through the potential lack of transparency into provider process and procedure environments.
- How to avoid service hijacking, where phishing, fraud and exploitation are well known issues in IT
- How to manage multi-instances in multi-tenancy virtual environments, when all instances are assumed isolated from each other. However, the assumption breaks down when attackers are able to cross virtual machines. Using side channels they can escape the boundaries of the sandboxed environment and have full access to a host.
- How to develop appropriate law and implement legal jurisdiction, so that users have a chain of evidence against their providers when required.

The survey by Aleem & Sprott, (2012) showed that the top concerns for organizations regarding cloud computing were security, governance and a lack of control over service availability. The survey highlighted that the majority of IT professionals were not aware that some CSPs currently control the decryption keys that enable them to decrypt their client's data. It could be considered as a major security concern and it is one of the factors that should be looked into at service level agreement (SLA) level. Data loss and leakage were nominated as the top threat to cloud computing by respondents; this was followed by account, service and traffic hijacking.

2.2 Cloud Privacy Issues

Privacy is the ability of an individual or group to control themselves or information about themselves and thereby reveal themselves selectively. Privacy issues in cloud computing environments can be divided into three sub-categories, which include (Nepal & Pathan, 2014):

- When a subject may be more concerned about the current or future information being revealed than information from the past.
- When a user may be comfortable if friends can manually request his information, but may not want alerts sent automatically.
- A Cloud user may rather have the information reported as an ambiguous region rather than a precise point.

In addition, the privacy issues differ according to different cloud scenarios (Xiao & Xiao, 2013), and can be divided into four subcategories as follows:

- How to make users remain control over their data when it is stored and processed in the cloud, and avoid theft, nefarious use and unauthorized resale.
- How to guarantee data replications are in a fixed jurisdiction, a consistent state, and has no data loss, leakage and unauthorized modification or fabrication.
- Identification of the party that is responsible for ensuring legal requirements for personal information.
- Cloud sub-contractors involved in processing can be identified, checked and verified.

2.3 Cloud Trust Issues

Trust is a measurable belief that utilizes experience, to make decisions. It is used in social science in constructing a human relationship and is now an essential substitute for forming security mechanisms in distributed computing environments. It has many soft security attributes, such as, reliability, dependability, confidence, honesty, belief, trustfulness, security, competence, and so on (Manuel, 2015). The security concern has different levels of trust in the different deployment models of cloud computing, due to the difference levels of trust among the communicating parties (Shaikh & Sasikumar, 2015). Trust in the private cloud computing model is expected to be at the highest level as the infrastructure and the assets will be managed and used by specific and well-known

entities. In the community cloud computing model, the cloud consumers (CCs) are from different organizations, and they will have the same level of security requirements. The trust level here may be lesser than the trust level in the private cloud, yet it is still better than the public cloud model. The problem of trust is in the public cloud computing model, in which the communication entities are unknown to each other is critical for transaction. However, it is the service provider's responsibility to build trust with its clients. Trust is the most complex relationship among entities because it is extremely subjective, context-dependent, non-symmetric, uncertain, and partially transitive (Chann & Chieu, 2010). Trust evaluation is a multi-faceted and multi-phased phenomenon based on multi-dimensional factors and the trust evaluation cycle. It is used to find the answer to the question "With which service providers should I interact and with which I should not?"

Trust issues in cloud computing environments can be divided into four sub-categories (Bezzi, Kalavuri & Sabetta, (2011) which include:

- How to define and evaluate trust according to the unique attributes in cloud computing environments.
- How to handle malicious information when trust relationships in clouds are temporary and dynamic.
- How to consider and provide a different security level for service according to the trust degree.
- How to manage trust degree change with interaction time and context, and to monitor, adjust, and to accurately reflect the trust relationship dynamic.

2.4 Cloud Monitoring Issues

Cloud Computing has a number of positive aspects pushing for its rapid adoption, from both the economic and the technical perspectives (Tormo, Marmol & Perez, 2012). The Cloud provides a lower Total Cost of Ownership, and increased flexibility in terms of both resources and Service Level Agreements. It allows for the focusing on the core business, by ignoring the costs related to infrastructure management. It also provides an improved scalability, ubiquitous access to data and resources, and advanced disaster recovery mechanisms. Together with these positive aspects Cloud Computing has a number of challenges for which the research community and industry are investing resources. Monitoring issues in cloud computing environments can be divided into four sub-categories (Dondio & Longo, 2011). The requirement is for accurate and fine-grained monitoring, platforms and measurement techniques.

- How to best monitor and measure provision of scalability, load balancing, Quality of Service (QoS), service continuity and application performance.
- How to guarantee SLAs.
- How to realize best measurement for management of large scale, complex and federated infrastructures.
- How to evaluate the root causes of end-to-end performance.

3 Cloud Identity

Effective cloud management recognises the need to use identity and advanced identity management mechanisms to overcome many of the issues noted in section 2. Identity management systems provide authentication and authorization based on end user identities. They keep privacy, while at the same time provide interoperability across multiple domains. Traditional identity management systems allow the end users, to some extent, to manage their personal information for accessing certain services. However, cloud computing brings a different perspective related to the end users' interests. Additionally, end users are more concerned about who can access their data. Identity management systems have been shown to be secure and efficient in diverse contexts and scenarios. By establishing trust relationships between providers and domains, identity management systems offer a huge range of features both for end users and for organizations regarding controlling and exchanging identity-related information while maintaining the privacy (Fang et al., 2012).

The user-centricity and privacy-preserving features offered by identity management systems, are key elements in cloud computing environments. Cloud computing integrates technologies and concepts from other fields, such as multi party computation, distributed systems, federation, and so on; and hence

some of the issues have already been addressed in other contexts, where identity management systems have been widely accepted (Fito & Guitant, 2014). Nevertheless, cloud computing brings a different perspective related to the end users interests, and delivers new risks for end user identities. Additionally, end users are more concerned about how their data is managed, where it is located and who can access it. In this sense, cloud computing is changing some of the basic assumptions (Fournaris & Keramidas, 2014).

To ensure the security of critical and sensitive data for customers the trust between Cloud identity providers has to be established before redirecting the customer's requests from one identity provider to another provider. Among all the cloud security issues, the ability to generate a trust value metric for identity management in the cloud is the most helpful to the end user. It is desirable that the users in one domain are able to access applications hosted in other clouds when a trust relationship already exists between the two cloud environments. Therefore, functionalities to manage the flow of user identity across clouds or domains are required. For this reason, a robust identity management (authentication, authorization and attribute data) must be put in place for cloud deployment and interaction in a usable and secure way. Likewise, the need for better access control and identity management systems as a main target for Federated Identity Management (FIM) plays a vital role in allowing the global scalability that is required for the successful implantation of cloud technologies. Current FIM frameworks are limited by the relative complexity of the underlying trust models and the complexity of the problem. Current FIM systems lack mechanisms to achieve dynamic federation, which is still an open challenge that requires further investigation (Garg et al., 2013). Thus, the establishment of dynamic federations between the different cloud identity actors is still a major theoretical challenge that has remained unsolved.

3.1 Cloud Identity Management System

Identity management systems were designed with the aim of providing an access control architecture, capable of preserving the users' privacy and enabling Single Sign-On by establishing trust relationships between different organizations. Shibboleth (Ghazizadeh, et al. (2014) and Liberty Alliance (Habib et al., 2012) are widely extended examples of identity management systems. In these systems, users' information is stored on reliable entities, named identity providers. Identity providers are in charge of managing users' identities, releasing required information to external entities. Service providers delegate the authentication process to identity providers, which in turn respond by sending the users' information on successful authentication. Additionally, they enable Single Sign-On, allowing users to access different services using their unique account. A set of commonly used mechanisms are reviewed below. The different approaches show the benefits of each in regards to the cloud identity system access. The federation establishment requires a metadata provider exchange; where the metadata contains identifiers, public key certificates, and service attributes. They are used for the location and secure communication between provider services. This decoupling between providers enables that IdPs can support many SPs in a distributed fashion, and also focus on managing identities, access control policies, and security token issuing.

The OAuth mechanism defines a protocol in order for clients to access server resources on behalf of a resource owner (Habib et al., 2012). It provides a process for end users to authorize third-party accesses to their server resources without sharing their credentials. Windows CardSpacealso known as its codename InfoCard, is the Microsoft client or Identity Selector for the Identity Metasystem (Habiba et al., 2014). Taking into consideration that the end users may have different identities depending on the context where they are interacting, the challenge of this approach is to allow the end users to create, use, and manage their diverse digital identities in an understandable and effective way. The idea behind Windows CardSpace is that end users could manage their digital identities, and their related attributes, in a similar way that they manage their cards in their wallets. When end users create an account in an OpenID identity provider, they receive an identifier as a URL or XRI. Then, when they access a relying party or service provider website which requires authentication and supports OpenID, they may enter their identifier in order to be redirected to their OpenID provider (Kanwal et al., 2014).

Yang et al. (2010) have an open source identity framework designed to enhance the end user experience, by integrating identity profiles and social relationships information across multiple sites. It not only manages end users' attributes, but it also manages data flows to external businesses and to other end users' personal data service. Luhmann (2000) is a cryptographic technology which presents a type of credential or token to encode end users' attributes in such a way that the issuance and the presentation of such tokens remains un-linkable. The technology makes use of Zero-knowledge proof methods to issue the tokens so that an end user can prove possession of a certain piece of information without revealing the information. Luo et al. (2012) is an anonymous credential system following the protocols

in order to allow the end users to control the dissemination of personal information and preserving their privacy. It allows where an end user can obtain credentials containing attested attributes from identity providers, and prove to a service provider the validity of such attributes without revealing any other information. OpenID Connect (Manuel, 2015) is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the end user in an interoperable and accurate manner. The functionality and workflow is shown in figure 2.

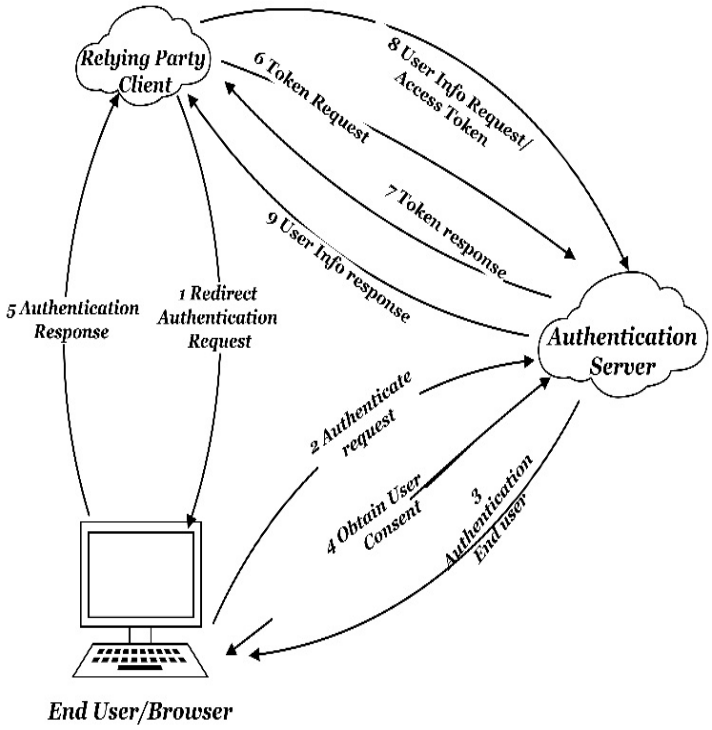

Figure 2: OpenID Connect General workflow (Manuel, 2015, p.14)

In the common workflow of SAML (Needleman, 2004), an end user wants to access a service from a service provider, but this service provider needs to authenticate the end user and obtain some attributes about the user. The authentication process, instead of being performed by the service provider, is delegated to the identity provider, which is in charge of managing the user's identity.

4 Trust Model and Mechanisms

Security is the dominant term when it comes to protection of sensitive data, but trust is a much stronger concept that goes beyond confidentiality, availability, integrity, and nonrepudiation (the basic security pillars). Trust formulates a good-faith relationship between computing machines as well as between their users. From the IT perspective, trust is not only about securing the communication channel or authenticating the data sender but also on trusting that the sent information are legitimate, they do not include malicious codes and they will not harm the receiver in an unforeseen way. In other words, trust extends to the sender itself by believing that they will obey to specific communication rules and will not abuse communication by non-responsiveness or selfish behavior (Napal & Pathan, 2014).

Trust and Reputation Rahman & Hailes (1998) are two indisputably recognised and relevant factors in human societies. Studies of trust have been carried out in different fields: psychology, sociology, economy and philosophy. Computational models of trust emerged in the last decade with the aim of exploiting the human notion of trust in open and decentralized environments. According to Noor & Sheng (2011), trust is adopted by humans to decrease the complexity of the society we are living by using delegation. Trust has emerged as a key element in decision-support solutions by helping agents in the selection of good and trustworthy collaborative partners, in the identification of reliable pieces of information or as part of soft-security applications. Trust is a concept borrowed from the human society and has different definitions in different fields. Properties of trust also vary from context to context. Here are some extracted properties commonly applied in computer science. Trust, in general, is not

transitive (non-transitive). Namely, if agent A trusts B and B trusts C, it is not possible to conclude that A also trusts C. However, under some conditions, A can trust C (Pagliere & Castlelfranchi, 2014). Secondly, trust is typically asymmetric. A member may trust another member more than she (he) is trusted back. However, when both parties are trustworthy, they will come to a high mutual trust level after repeated interactions. Conversely, if one of the members does not act in a trustworthy manner, the other member will be forced to penalize him/her, leading to low mutual trust. Asymmetry can be considered a particular case of personalization (Paglieri, 2013). Thirdly, trust value may change over time as a dynamic factor. The most recent value of trust is more informative and persuasive in decision-making. Due to the dynamic behaviour of agents, the trustworthiness of an agent may change over time. Thus, it needs to be updated. Fourthly, trust is subjective and self-reinforcing dynamic which means when a cloud user chooses to trust or distrust a provider, it is a personal choice. Each user has its own preference or interests (subjectivity) that influence their trust reasoning (Qu, Wang & Orgun, 2013). Finally, trust is context-aware. It means different scenarios have different types of trust (Radha & Reddy, 2012).

A typical computational trust solution follows the high-level architecture shown in (Sakimura et al., 2014). In a typical distributed environment, an agent (trustier) is acting in a domain where the trustier needs to trust other agents or objects, whose ability and reliability are unknown. The trustier agent queries the trust system to gather more knowledge about the trustee agent and in order to better ground decisions. A trust-based decision in a specific domain is a multi-stage process. The first step is the identification and selection of the appropriate input data. These data are in general domain-specific and identified through an analysis conducted over the application.

Evidence selection is driven by an underlying trust model that contains the notion of trust on which the entire system is centred. A trust model represents the intelligence used to justify which elements are selected as trust evidence, why some elements are selected and other discarded, and it informs the computation over the selected evidence. A trust model contains the definition of the notion of trust, its dynamics, how it evolves over time and with new evidences, and the mechanisms of trust used in the computation. After evidence selection, a trust computation is performed over evidence to produce trust values. This is the estimation of the trustworthiness of entities in a particular domain. A trust computation requires the formalization of a computable version of those mechanisms defined in the trust model. Examples of such mechanisms are the past-outcomes, reputation and recommendation, but also temporal and social factors, similarity, and categorization. For instance, a classical trust system uses two sets of evidence: recommendations and past experience. Each of them is quantified separately and then aggregated into a final value. In this final aggregation stage, exogenous factors such as risk and trustier' s disposition can also be considered. The output is presented as quantitative trust values and as a set of justifications.

4.1 Evaluation of System Architecture

The components of the trust framework adapted from Shaikh & Sasikumar, (2013) are in figure 3. In order to generate successful collaborated applications, a trust mechanism is incorporated. A node's trust value is assessed based on direct observations and indirect information from recommendations. The trust of one node toward another node is updated upon an encounter and interaction events. Each node will execute the trust protocol independently and will perform its direct trust assessment toward an encountered node based on specific detection mechanisms designed for assessing the trust property. This framework provides features such as service selection based on trust requirements and ranking of distributed computing based on previous user experiences and real time performance. The key elements are:

- Cloud entities: This component is responsible for interaction with customers and understanding their application needs, and performs discovery and ranking of suitable trusted services using other components such as the trust management, direct/indirect trust and evaluation method.
- Monitoring and history information: this component first discovers services that can satisfy users' needs. Then, it closely monitors the trust performance of the services, such as direct and indirect trust. At the same time, related history records are stored in service database.
- Computing service network structure and catalogue: builds the service network and their features advertised by various different providers, divides computing resources into different classes.

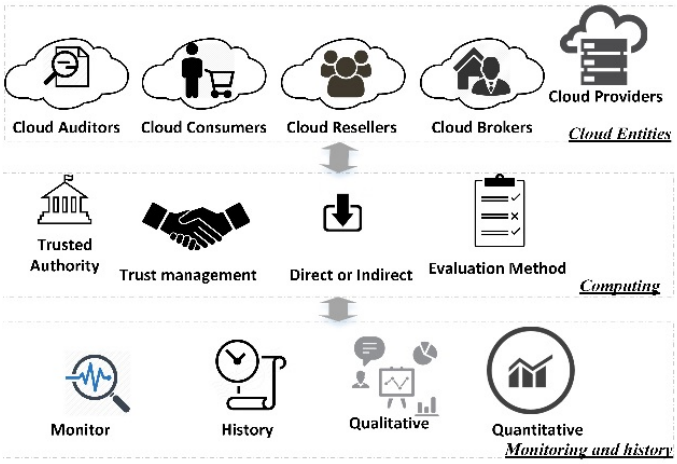

Figure 3: Service Trust Evaluation System Architecture (adapted from Shaikh & Sasikumar, 2013)

4.2 Trust Establishment

The taxonomies for functional and non-functional features in a trust model (Schryen et al., 2011) can be used as an assessment criterion to evaluate the existing trust models in the Cloud domain. The non-functional features include, security, performance, control, and deployment of the model. The functional features include the agreements made, certificates issued, feedback given, domain of operation, and the subjectivity of the decision-making model. Service level agreement (SLA) based trust model (STM) (Shaikh & Sasikumar, 2013) and Trust model for security aware Cloud (TMSAW) (Shaikh & Sasikumar, 2015) are two examples of the agreement-based trust models which the SLA plays a primary role in trust evaluation of cloud service providers. In the STM, the SLA agents are responsible for asserting the required parameters of encryption and key management, hence providing data confidentiality. The SLA-management module in SLA-agent is responsible for creating and negotiating the access control policies for data stored in the Cloud, thus guaranteeing the data ownership to customers. This model does not encounter any procedure to assure the process execution control, which is an important attribute for elevating the trust level on a CSP. In addition, the SLA-agent manages and inserts the necessary parameters for data replication in SLAs, thus assuring data availability. The Trust management module collects feedback (from external Cloud providers) that is used to analyse the QoS transparency offered by a specific CSP. Detection of malicious entities is obtained via credibility weights, which are assigned to the sources of information and the aggregated value is calculated. SLA-agents need to design and select the required parameters for the SLAs while creation and management related tasks are performed by the CSP. The functionality of the model can be enhanced by introducing a new module that can be easily integrated with SLA reports to obtain better and more reliable trust values, and high flexibility. The STM does not support a dynamic update of the SLA parameters and is, therefore, considered to be passive for the Cloud environment. The model is capable of evaluating the Cloud services, but does not facilitate the trust evaluation of the Cloud consumers and therefore, does not support the dual root of trust. Nevertheless, the parameter monitoring module of the SLA agent continuously observes and monitors the SLA attributes to avoid any inconsistency and inaccuracy in the trust score formulation.

Ahmed et al. have proposed a Ticket-based trust model (TTM) to establish trust on the Cloud providers. TTMs are issued by the data owner for authorized users, where capability lists (user-id, data-id, access rights AR) define the access rights of users on data stored on the Cloud, thus assuring the data ownership offered by the CSP. The model does not provide any mechanism to ensure the process execution control in the Cloud. Likewise, no mechanism is adopted to evaluate the QoS transparency presented by the CSP. A Certification-based trust model (CTM) [48] does not provide any mechanism to assure the process execution control and the QoS transparency. Moreover, the dynamic composition of services introduces high complexity in implementation of the discovery framework. The required number of Cloud services can be examined and validated from the certificates issued by accreditation authorities, thus introducing high flexibility in the model. Moreover, the framework can select the Cloud service accredited by third parties to satisfy the data replication that assures data availability.

5 Trust Frameworks

Selecting the best cloud service from the available cloud providers is a complex and challenging task for the cloud users. There is a multitude of works that employ optimization to achieve this goal. However they limit the applicability of the method to generalise and usually require select input data that structures a view of a current situation. Other models are required that can compensate for many of the ambiguity is found in cloud environments. For the end user to identify trustworthy cloud services is difficult because much of the evidence is not available to them. Consequently the concept of the trust framework in which generalise guidelines and specific metrics are found can be a useful tool in this type of decision-making. Table 1 provides an analysis from literature of trust frameworks into six categories: risk, authentication, security, accuracy, integration, and privacy.

Trust Framework	Risk	Authentication	Security	Accuracy	Integration	Privacy
Fang, et al., 2012.	QL	A	SC,SA	N	N	N
Tanimoto et al., 2011.	QL	N	SA	N	N	PP.PC
Theoharidou et al., 2013.	QQ	N	SC	N	N	PC
Tormo et al., 2014.	QQ	A	SC,SA	N	N	PP,PC
Vullers & Alpar, 2013.	QL	N	SA	N	N	N
Wagle et al., 2015.	QL	Ni	SA,SC	AF,AA	N	PC
Wang et al., 2015.	QQ	N	SA,SC	AF,AA	I	PC
Wei et al., 2014.	N	N	SC	N	I	PP
Aleem & Sprott, 2012.	QL	N	SA,SC	N	N	PP
Lyaniv & Kleinberger, 2000.	N	N	SA,SC	N	I	PP
Yeluri & Leon, 2014.	N	N	SC	N	N	N
Zhuang et al., 2012.	N	A	SA,SC	N	N	PP
Zhuang et al., 2010.	QL	A	SA	N	N	N
Schryen et al., 2011.	N	N	SC	AF	I	PP
Zheng et al., 2013.	N	N	SC	AF	I	N
Qu et al., 2013	N	N	SC	AF	I	N

Table 1. Comparison of existing cloud trust frameworks (Mnemonics in text)

The first category of analysis is risk. Different trust frameworks supply a different conception and methodologies for the calculation of risk. For example, the approaches can be grouped under the three risk assessment methods: quantitative (QN), qualitative (QL), and semi-quantitative (QQ). The second category for analysis is Authentication (A). These mechanisms are used to establish consumers' identities when registering for a service. The analysis of these mechanisms give evidence on which to make a trust based decision. The third category is Security (S). The security mechanisms employed by a cloud service also hint at its trustworthiness. An assessment requires appropriate security mechanisms at both the access control (SA) and communication (SC) levels. Privacy (P) is another factor in determining the trustworthiness of a service. Knowing a cloud service's privacy policy can help determine whether to trust that service with essential data. Based on SLAs, privacy responsibility can be split between the provider (PP), who deploys all necessary security measures, and consumers (PC), who take their own steps to preserve data privacy. The fourth criteria is Accuracy. The accuracy of trust assessment depends on both the correct identification of trust feedback and effective assessment function security. Poor identification of trust feedback (AF) and/or failure to prevent attackers (AA) from manipulating trust results can lead to inaccurate results in trust management systems. Combining several techniques like reputation and recommendations can increase trust results' accuracy; Integrity

(I) may also lead to better trust results by matching appropriate consumers to trustworthy providers (Toromo, Marmol & Perez, 2014).

These criteria have been used to evaluate representative trust management systems for cloud computing and related areas such as grid, P2P, and service-oriented computing. The analysis yielded several open research challenges. Cloud users are the real owner of the data assets, thus, ignoring their business objective will result in an inaccurate evaluation of cloud provider trust level. The most popular risk assessment standards, such as NIST SP800-30 assume that an organization's assets are fully managed by the organization itself. This is not the case for cloud computing model. Moreover, a big problem today is that, all too often, different CSPs or CIdPs employ their own jargon to describe risk, while at the same time measuring its impact and the probability that it will manifest itself is expressed in a subjective fashion. Therefore, as a starting point, risk assessment will bring a common framework for managing different types of risk in the same way.

6 Discussion

Cloud computing involves many security risks, which may require the re-evaluation against a new set of criteria. Therefore, security risk assessment in cloud computing requires further research to develop an appropriate risk assessment methodology. For scalability reasons, trust relationships between the CIdP, CIdU, CSP should be assessed as on-demand instead of statically. Such a move would bring quality improvement to the methods currently applied for Cloud identity. However, there is a high uncertainty component when deciding whether to cooperate or not with unknown providers. Hence, there is an ongoing project to identify the risks associated with the Cloud computing paradigm. Risks associated with the virtualization technology, such as failures in multi-tenancy, virtual machine (VM) isolation, and hypervisor vulnerabilities; loss of direct control of resources and software such as provider lock-in, decreased reliability since providers may go out of business, agreement (SLA) breaches; risks associated with data such as data protection responsibility, insecure or incomplete data deletion; and legal risks such as regulatory compliance, data location, and the effect of international boundaries on operation: are some of the risks that cloud computing has introduced. Thus, every CIdU has to make decisions that imply dealing with some form of risk. CIdU may request evidence to determine if it is secure to collaborate with a particular unknown CIdPs.

The end user trust can be improved when choosing an identity service by greater transparency and clarity on the part of the CIdP. Similarly, a CSP has to decide if it is sufficiently secure to accept authentication statements or other identity data issued by a specific CIdP. It is also crucial that users are aware of the transactions regarding their identity. In fact, they should be provided with risk information to determine if they should reveal their personal data to the CSP or CIdP. Public-key infrastructure (PKI), access management services, Rule-based access control, password based protection, and Secure Shell (SSH) are examples for cloud authentication from which vital evidence may be gained to populate the trust model. Further differentiation is required of the applicability of trust assessment functions for each service provider. A greater number of authentication types equates with a high level of trust.

Most of the trust models reviewed do not use any mechanism to identify authentic trust feedback. This is a significant challenge in the cloud because of the overlapping interactions between service providers and consumers. Also most of the trust management systems have been analyzed do not have a mechanism to preserve participants' privacy, highlighting the urgent need for efficient techniques that protect users' privacy while minimizing the impact to system performance. Importantly, most of the trust management systems examined do not support the integration of trust feedback for the end user to view. Techniques that can efficiently integrate trust feedback is needed to improve trust results. Again most of the trust management systems that have been evaluated do not provide security at the access control and communication level. However, attacks can come from system users themselves. The situation is accentuated in cloud environments due to the dynamic interactions and the distributed nature of cloud services, which make it difficult to identify attackers. Mitigation techniques are required to enhance end user trust. Some of the works, compared the low-level performance metrics of Cloud services such as CPU utilization and network throughput. Such low-level performance metrics can be further used to create models of high-level system properties, such as power consumption and performance. Weightings can be added to reflect each service provider protective mechanism capability and the provision of the different attributes such as security, privacy, and performance measurements.

Considerable literature exists on trust models in Cloud computing that evaluates the trust of Cloud services. The detailed analysis concludes that all the trust models in Cloud computing are mainly designed to evaluate the trust between Cloud CS and CSPs. None of these trust models focus on evaluation and establishment of trust in the inter-Cloud domain; thus the Cloud federation lacks trust

evaluation approaches and techniques. After analysing these trust models, it is further concluded that trust evaluation should not be based on single factor (feedback, SLA or recommendation) rather a trust value should be the aggregation of these different factors. Keeping in view the potential growth of Cloud federation and the need for trust evaluation model to achieve the trusted federation (Kanwal, Masood, & Shibli, 2014), a trust evaluation model that is based on two essential factors of feedback and QoP attributes in SLAs is required. From this model a single metric may be generated for end user trust.

As an outcome for the literature survey, it is noted at there are few research articles that focus on the evaluation of cloud identity providers or on finding appropriate solutions to establish confidence and trust between the consumers and the cloud identity provider. The implications for trust frameworks are that the start on any proposal will be with an inadequate literature foundation. Guidelines for evaluating trust in the cloud environment need to begin with a fresh assessment of the context and a recognition of the differences between a cloud environment context and all previous computing contexts, including grid networks.

At present there are no unified standards or metric frameworks that span the cloud context. The evaluation of trust, the building of trust models, and the design of trust frameworks can decrease the complexity of the cloud environment by delegating decision-making to measurable attributes within the systems framework. To evaluate the trust of service nodes scientifically needs a new framework and evaluation method to determine the weight of different indexes, and fully reflect the objectivity and accuracy in cloud authentication contexts. The outstanding problem is that current research of trust evaluation is still in its infancy, and it still has a considerable problem space to explore and to resolve. The end user requires less information and more evidence that their information is secure. The required evidence is a holistic grouping from multiple factors that is to be accessible for decision-making. A whole evaluation framework for trust evaluation, is required which can help users choose and to monitor the cloud identity provider states and demonstrations of trusted behavior. Some of the metrics would include trust effectiveness measures such as uncertainty, aggregation and customization. Moreover, there is no framework that can allow CIdUs to evaluate CIdPs services and rank them based on their ability to meet the CIdU's requirements. A Cloud trust framework is a desirable innovation but challenges still remained for security, privacy, access control, and integration; and these continue to be major weaknesses inhibiting cloud end user decision making.

7 Conclusion

The end user of Cloud services requires greater evidence on which to base trusting decisions regarding service supply. The complexity of the situation is compounded by the nature of the cloud environment that allows a service supplier to move between contractual arrangements and jurisdictions regardless of where the end user may be located. In the literature reviewed a gap was identified around the evaluation of trust and its attributes in Cloud services. Several solutions were reviewed that provide metrics to determine the credibility of trust in cloud environments. The trust value metric is particularly useful once the assessment methodology is a formalized. The focus on cloud identity was selected as this is a key area where privacy and security are critical. The unpredictable number of cloud service consumers and highly dynamic nature of cloud environments accentuate the problem of intercommunicating obstacles occurring among CIdPs and CIdUs. The evidence an end user looks for, can be compiled from a fair assessment of service provider attributes and their security mechanisms. Trust-based modelling provides a solution from which a trust framework may be developed to assure a trustworthy foundation for decision-making. Further research is required into optimal framework architectures, the assessment criteria and the adequacy of feedback and review loops. Also the composition of trust models ought to be open for evaluation so the relative strengths and weaknesses of each may be reported to the end user as part of the evidence on which decisions may be made.

8 References

Abdul-Rahman, A., & Hailes, S. (1998). A distributed trust modelACM. Symposium conducted at the meeting of the Proceedings of the 1997 workshop on New security paradigms

Aceto, G., Botta, A., De Donato, W., & Pescapè, A. (2013). Cloud monitoring: A survey. Computer Networks, 57(9), 2093-2115.

Ahmed, M., & Xiang, Y. (2011). Trust Ticket Deployment: A Notion of a Data Owner's Trust in Cloud ComputingIEEE. Symposium conducted at the meeting of the Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on

Albakri, S. H., Shanmugam, B., Samy, G. N., Idris, N. B., & Ahmed, A. (2014). Security risk assessment framework for cloud computing environments. Security and Communication Networks, 7(11), 2114-2124.

Aleem, A., & Ryan Sprott, C. (2012). Let me in the cloud: analysis of the benefit and risk assessment of cloud platform. Journal of Financial Crime, 20(1), 6-24.

Alhamad, M., Dillon, T., & Chang, E. (2010). Sla-based trust model for cloud computingIEEE. Symposium conducted at the meeting of the Network-Based Information Systems (NBiS), 2010 13th International Conference on

Alhamazani, K., Ranjan, R., Mitra, K., Rabhi, F., Jayaraman, P. P., Khan, S. U. (2015). An overview of the commercial cloud monitoring tools: research dimensions, design issues, and state-of-the-art. Computing, 97(4), 357-377.

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information Sciences, 305, 357-383.

Ardaggna, C.,Etisalat,R.,Vu,Q. 2015. From security to assurance in the cloud: a survey. ACM computing surveys, 48, 1, 2-50.

Benlian, A.,Hess, T. (2011). Opportunities and risks of software-as-a-service: findings from a survey of IT executives, Decision Support Systems, 52(1), 232–246.

Bezzi, M., Kaluvuri, S. P., & Sabetta, A. (2011). Ensuring trust in service consumption through security certificationACM. Symposium conducted at the meeting of the Proceedings of the International Workshop on Quality Assurance for Service-Based Applications.

Cabarcos, P., Almenárez-Mendoza, F., Marín-López, A., Díaz-Sánchez, D., & Sánchez-Guerrero, R. (2012). A metric-based approach to assess risk for “on cloud” federated identity management. Journal of Network and Systems Management, 20(4), 513-533.

Chan, H., & Chieu, T. (2010). Ranking and mapping of applications to cloud computing services by SVDIEEE. Symposium conducted at the meeting of the Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP

Dondio, P., & Longo, L. (2011). Trust-based techniques for collective intelligence in social search systems. In Next Generation Data Technologies for Collective Computational Intelligence (pp. 113-135): Springer.

Fang, H., Zhang, J., Şensoy, M., & Thalmann, N. M. (2012). SARC: subjectivity alignment for reputation computationInternational Foundation for Autonomous Agents and Multiagent Systems. Symposium conducted at the meeting of the Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems-Volume 3

Fitó, J. O., & Guitart, J. (2014). Business-driven management of infrastructure-level risks in Cloud providers. Future Generation Computer Systems, 32, 41-53. doi:http://dx.doi.org/10.1016/j.future.2012.05.008

Fournaris, A. P., & Keramidas, G. (2014). From Hardware Security Tokens to Trusted Computing and Trusted Systems. In System-Level Design Methodologies for Telecommunication (pp. 99-117): Springer.

Garg, S. K., Versteeg, S., & Buyya, R. (2013). A framework for ranking of cloud computing services. Future Generation Computer Systems, 29(4), 1012-1023.

Ghazizadeh, E., Shams Dolatabadi, Z., Khaleghparast, R., Zamani, M., Manaf, A. A., & Abdullah, M. S. (2014). Secure OpenID authentication model by using Trusted ComputingHindawi Publishing Corporation. Symposium conducted at the meeting of the Abstract and Applied Analysis.

Goode, S., Lin, C., Tsai, J. C., Jiang, J. (2015). Rethinking the Role of Security in Client Satisfaction with Software-As-A-Service (Saas) Providers, Decision Support Systems, 70, 73-85.

Habib, S. M., Hauke, S., Ries, S., & Mühlhäuser, M. (2012). Trust as a facilitator in cloud computing: a survey. Journal of Cloud Computing, 1(1), 1-18.

Habib, S. M., Ries, S., & Mühlhäuser, M. (2011b). Towards a trust management system for cloud computingIEEE. Symposium conducted at the meeting of the Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on

Habiba, U., Masood, R., Shibli, M. A., & Niazi, M. A. (2014). Cloud identity management security issues & solutions: a taxonomy. Complex Adaptive Systems Modeling, 2(1), 1-37.

Kanwal, A., Masood, R., Shibli, M. A., & Mumtaz, R. (2014). Taxonomy for Trust Models in Cloud Computing. The Computer Journal, bxu138.

Li, A., Yang, X., Kandula, S., & Zhang, M. (2010). CloudCmp: comparing public cloud providers. ACM Symposium conducted at the meeting of the Proceedings of the 10th ACM SIGCOMM conference on Internet measurement.

Luhmann, N. (2000). Familiarity, confidence, trust: Problems and alternatives. Trust: Making and breaking cooperative relations, 6, 94-107.

Luo, C., Zhan, J., Jia, Z., Wang, L., Lu, G., Zhang, L.,. Sun, N. (2012). Cloudrank-d: benchmarking and ranking cloud computing systems for data processing applications. Frontiers of Computer Science, 6(4), 347-362.

Manuel, P. (2015). A trust model of cloud computing based on Quality of Service. Annals of Operations Research, 233(1), 281-292.

Needleman, M. (2004). The Shibboleth authentication/authorization system. Serials Review, 30(3), 252-253.

Nepal, S., & Pathan, M. (2014). Security, Privacy and Trust in Cloud Systems. Springer: New York.

NIST. (2013). Final Version of NIST Cloud Computing Definition Published. Retrieved from http://www.nist.gov/itl/csd/cloud-102511.cfm

Noor, T. H., & Sheng, Q. Z. (2011). Trust as a service: a framework for trust management in cloud environments. In Web Information System Engineering–WISE 2011 (pp. 314-321): Springer.

Noor, T. H., Sheng, Q. Z., Maamar, Z., & Zeadally, S. 2016. Managing Trust in the Cloud: State of the Art and Research Challenges. Computer, 49(2), 34-45.

Noor, T., Sheng, Q., Zeadally, S. and Yu, J. 2013. Trust management of services in cloud environments: obstacles and solutions. ACM Computing Surveys 46, 1, 12-30.

Oliveira, T., Thomas, M., Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: an analysis of the manufacturing and services sectors, Information & Management, 51(5), 497–510.

Paglieri, F., & Castelfranchi, C. (2014). Trust, relevance, and arguments. Argument & Computation, 5(2-3), 216-236.

Paquin, C. (2013). U-Prove Technology Overview V1. 1 (Revision 2). Microsoft, White Paper.

Pearson, S. (2013). Privacy, security and trust in cloud computing. In Privacy and Security for Cloud Computing (pp. 3-42): Springer.

Qu, L., Wang, Y., & Orgun, M. A. (2013). Cloud service selection based on the aggregation of user feedback and quantitative performance assessment. IEEE. Symposium conducted at the meeting of the Services Computing (SCC), 2013 IEEE International Conference on

Radha, V., & Reddy, D. H. (2012). A survey on single sign-on techniques. Procedia Technology, 4, 134-139.

Ramesh, R., & Zionts, S. (2013). Multiple criteria decision making. In Encyclopedia of Operations Research and Management Science (pp. 1007-1013): Springer.

Ray, I., Ray, I., & Chakraborty, S. (2009). An interoperable context sensitive model of trust. Journal of Intelligent Information Systems, 32(1), 75-104.

Roy, A., Sarkar, S., Ganesan, R. and Goel, G. 2015. Secure the cloud: from the perspective of a service-oriented organization. ACM Computing Surveys 47, 3, 41-71.

Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., & Mortimore, C. (2014). Openid connect core 1.0. The OpenID Foundation, S3.

Sato, H., Kanai, A., & Tanimoto, S. (2010). A cloud trust model in a security aware cloud. IEEE. Symposium conducted at the meeting of the Applications and the Internet (SAINT), 2010.

Schryen, G., Volkamer, M., Ries, S., & Habib, S. M. (2011). A formal approach towards measuring trust in distributed systemsACM. Symposium conducted at the meeting of the Proceedings of the 2011 ACM Symposium on Applied Computing.

Shaikh, R., & Sasikumar, M. (2013). Identity Management in Cloud Computing. International Journal of Computer Applications, 63(11).

Shaikh, R., & Sasikumar, M. (2015). Trust Model for Measuring Security Strength of Cloud Computing Service. Procedia Computer Science, 45, 380-389.

Shernan, E., Carter, H., Tian, D., Traynor, P., & Butler, K. (2015). More Guidelines than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations. In Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 239-260): Springer.

Sun, D., Chang, G., Sun, L., & Wang, X. (2011). Surveying and analyzing security, privacy and trust issues in cloud computing environments. Procedia Engineering, 15, 2852-2856.

Tanimoto, S., Hiramoto, M., Iwashita, M., Sato, H., & Kanai, A. (2011). Risk management on the security problem in cloud computingIEEE. Symposium conducted at the meeting of the Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference.

Theoharidou, M., Tsalis, N., & Gritzalis, D. (2013). In cloud we trust: Risk-Assessment-as-a-Service. In Trust Management VII (pp. 100-110): Springer.

Tormo, G. D., Mármol, F. G., & Pérez, G. M. (2014). Identity Management in Cloud Systems. In Security, Privacy and Trust in Cloud Systems (pp. 177-210): Springer.

Tormo, G., Mármol, F., & Pérez, G. (2012). On the application of trust and reputation management and user-centric techniques for identity management systems Symposium conducted at the meeting of the XII Spanish meeting on cryptology and information security (RECSI 2012), San Sebastián, Spain.

Vullers, P., & Alpár, G. (2013). Efficient selective disclosure on smart cards using idemix. In Policies and Research in Identity Management (pp. 53-67): Springer.

Wagle, S. S., Guzek, M., Bouvry, P., & Bisdorff, R. (2015). An Evaluation Model for Selecting Cloud Services from Commercially Available Cloud Providers.

Wang, L., Li, X., Yan, X., Qing, S., & Chen, Y. (2015). Service Dynamic Trust Evaluation Model based on Bayesian Network in Distributed Computing Environment. Distributed computing, 9(5).

Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., & Vasilakos, A. V. (2014). Security and privacy for storage and computation in cloud computing. Information Sciences, 258, 371-386.

Yaniv, I., & Kleinberger, E. (2000). Advice taking in decision making: Egocentric discounting and reputation formation. Organizational behavior and human decision processes, 83(2), 260-281.

Yeluri, R., & Castro-Leon, E. (2014). The trusted cloud: addressing security and compliance. In Building the Infrastructure for Cloud Security (pp. 19-36): Springer.

Zhang, H., Wang, Y., & Zhang, X. (2012). A trust vector approach to transaction context-aware trust evaluation in e-commerce and e-service environmentsIEEE. Symposium conducted at the meeting of the Service-Oriented Computing and Applications (SOCA), 2012 5th IEEE International Conference.

Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010). Information security risk management framework for the cloud computing environmentsIEEE. Symposium conducted at the meeting of the Computer and Information Technology (CIT), 2010 IEEE 10th International Conference.

Zheng, Z., Wu, X., Zhang, Y., Lyu, M. R., & Wang, J. (2013). QoS ranking prediction for cloud services. Parallel and Distributed Systems, IEEE Transactions on, 24(6), 1213-1222.

Copyright